NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

INFORMATION WARFARE TARGETING: PEOPLE AND PROCESSES

by

Ken Wang

December 2003

Thesis Advisor: Dan C. Boger
Co-Advisor: Raymond Buettner

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Information Warfare Targeting: People and Processes	**5. FUNDING NUMBERS**
6. AUTHOR(S) Lieutenant Commander Kenny Wang, USN	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Information Warfare targeting has long been a crucial, but unrecognized, part of military operations. From Sun Tzu's targeting of the enemy's will to fight, to today's information-centric warfare, it is those who have understood the techniques and applications of Information Warfare targeting who have most often prevailed. As critical as it is to our success, it is a topic that is controversial, often misunderstood, and subject to various interpretations.

This thesis examines the IW targeting process, consisting of people, information, systems, and the interaction between the function of targeting and IW. In the Information Age, IW has been recognized as viable warfare area. However, IW Targeting cannot be treated as traditional targeting utilized by other warfare areas. This thesis is intended to serve as a guide for the study of this topic and provides an instructional program designed to satisfy the requirement for a coherent instructional program on IW Targeting.

IW targeting affects every facet of warfare and in turn is affected by these facets. In preparing for a future that calls for maximizing the effects while minimizing the effort, it is critical that we understand the process in order to remain effective.

14. SUBJECT TERMS Command and Control Warfare, Effects Based Targeting, Information Warfare, Information Operations, Targeting	**15. NUMBER OF PAGES** 67
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

INFORMATION WARFARE TARGETING: PEOPLE AND PROCESSES

Kenny NMN Wang
Lieutenant Commander, United States Navy
B.S., University of Florida, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2003

Author: Kenny NMN Wang

Approved by: Dan C. Boger
Thesis Advisor

Raymond Buettner
Co-Advisor

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information Warfare targeting has long been a crucial, but unrecognized, part of military operations. From Sun Tzu's targeting of the enemy's will to fight, to today's information-centric warfare, it is those who have understood the techniques and applications of Information Warfare targeting who have most often prevailed. As critical as it is to our success, it is a topic that is controversial, often misunderstood, and subject to various interpretations.

This thesis examines the IW targeting process, consisting of people, information, systems, and the interaction between the function of targeting and IW. In the Information Age, IW has been recognized as viable warfare area. However, IW targeting cannot be treated as traditional targeting utilized by other warfare areas. This thesis is intended to serve as a guide for the study of this topic and provides an instructional program designed to satisfy the requirement for a coherent instructional program on IW Targeting.

IW targeting affects every facet of warfare and in turn is affected by these facets. In preparing for a future that calls for maximizing the effects while minimizing the effort, it is critical that we understand the process in order to remain effective.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Information Warfare targeting has long been a crucial, but unrecognized, part of military operations. From Sun Tzu's targeting of the enemy's will to fight, to today's information-centric warfare, those who have understood and applied the techniques and tools of Information Warfare targeting are those who have most often prevailed. As critical as it is to our success, it is a topic that is controversial, often misunderstood, and subject to various interpretations.

This thesis examines the Information Warfare targeting process, consisting of people, information, support systems, and the interaction between the functions of targeting. It is intended to serve as a guide for the study of this topic from a foundational standpoint by first exploring the doctrinal definitions used throughout DoD and developing a sense of what Information Warfare targeting is and is not. It then focuses on the components of the process and the dynamic relationships that exist between them. Finally, it attempts to develop a course of instruction aimed at the mid grade military officer, to facilitate the officer's understanding of Information Warfare and the integration of Information Warfare into the targeting process.

Information Warfare targeting affects every facet of warfare and, in turn, is affected by these facets. In preparing for a future that calls for maximizing the effects while minimizing the effort, it is critical that we understand the process in order to remain effective.

1. History of Targeting

As presented in *FM 90-36*, traditional ideas of targeting have always been to destroy or neutralize a target with conventional weaponry. With neutralization becoming a euphemism for physically damaging the target so that it cannot function effectively. Though Sun Tzu has written about warfare utilizing other than destruction as a tool, history has shown from the days of Sun Tzu to modern day warfare that conventional weaponry and destruction seem to be the rule.

> The invention of gunpowder and the constant improvement of firearms are enough to show that the advance of civilization has done nothing practical to alter or deflect the impulse to destroy the enemy, which is the central idea of war. – Clausewitz[1]

The idea of targeting an enemy to achieve a specific effect has existed in past strategic philosophy. Sun Tzu states, "Thus, what is of supreme importance in war is to attack the enemy's strategy."[2] Another example of this is from Captain Basil Liddell Hart, when he states, "The real target in war is the mind of the enemy commander, not the bodies of his troops."[3] The actual practice of targeting for an effect other than destruction or neutralization has been the exception, rather than the norm. Current ideas of effects based operations, as such effects based targeting, have always been in existence, however, the effects have usually been to either destroy or neutralize. The US military has excelled at this paradigm of conventional weaponry and destruction of the enemy. Only in the past 10-15 years have "revolutionary" ideas in military affairs brought forth a new philosophy to explore alternate means

to achieve the objective. We will see that today the effects available to achieve the commander's objectives have broadened in scope.

2. New Paradigms

With the formal recognition of Information Warfare and, more broadly Information Operations in *DOD Directive 3600.1*, traditional ideas of targeting must be revisited. As stated in Joint Publication 3-13, Information Operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems.[4] This line of thinking still relies on the old paradigm of targeting for destruction, only now the targets include the information and information systems. The underlying key idea that we must embrace is to go beyond the physical and look toward the effects, which this method of targeting entails. We will examine the new targets available, the new weapons, and tools to affect these new targets, with the key idea being to influence the enemy. As presented in *Joint Publication 3-13*, due to the old paradigms, IO targeting and planning have been disjointed and uncoordinated. IO targeting and plans have focused on the individual core competencies of IO without much consideration to other aspects of the operation or even the other core competencies. Targeting and planning "in a vacuum" is another old paradigm that must be set aside to fully realize the potential of an IO paradigm. The new paradigm seeks a coordinated effort of all the IO competencies in conjunction with all the other aspects of the operation to create a synergistic effect to achieve the objectives. The idea being, that the whole effect will be greater than the sum of its parts.

B. PURPOSE

The purpose of this thesis is to address the central themes of Information Warfare targeting. These themes include the idea of effects based targeting, current targeting processes and methodologies, and the integration of Information Warfare Targeting with traditional targeting processes.

Currently, there does not exist a unifying instructional program that embodies the new paradigms of Information Warfare Targeting. During the conduct of research for this project, course material in the form of readings, slide presentations, and case studies was compiled for use in the classroom. Also, a course of instruction was developed to address these new paradigms. The purpose of this course is to direct the thinking of the students from traditional targeting paradigms to exploring potentially new options for planning, target selection, and target-weapon-effect matching.

The entire course of instruction and supporting materials resides on Blackboard. Blackboard is an online aid to assist facilitation of a course. One objective is to be able to utilize Blackboard to facilitate distance learning. The rest of the material is located in a public folder and available on the classified SIPRnet LAN, at the Naval Postgraduate School. This document is intended to provide the reader an overview of topics and themes from the course material.

C. SCOPE

This thesis is aimed at the mid-grade military officer with a basic understanding of Information Warfare/ Information Operations and operational staff experience. It will focus primarily on developing an understanding of Information Warfare targeting and how it relates to the overall targeting process. The intent is to expose the readers to the new effects defined in current doctrine and available through new technologies, and to discuss how the doctrine and technologies will impact the traditional objectives of targeting. The course material provided on these subjects will require periodic updating to maintain the relevance of the material in this dynamic field. Though the field of Information Warfare/Information Operations is broad in scope, we will limit the scope of this document to the specific aspects of targeting and target-weapon-effect matching. The documents used will cover the spectrum from joint and service specific publications to articles with a special emphasis placed on those concerned with theater/operational level Information Warfare targeting theories and concepts.

THIS PAGE INTENTIONALLY LEFT BLANK

II. INFORMATION WARFARE

A. INFORMATION WARFARE CONCEPTS

Information Warfare is Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.[5] Information Operations involve actions taken to affect adversary information and information systems while defending one's own information and information systems.[6] Information Warfare can achieve effects in all other operational cultures, as such, it is also affected by those same operational areas. We will briefly cover the five core competencies (See Figure 1) and the supporting foundations of IW.

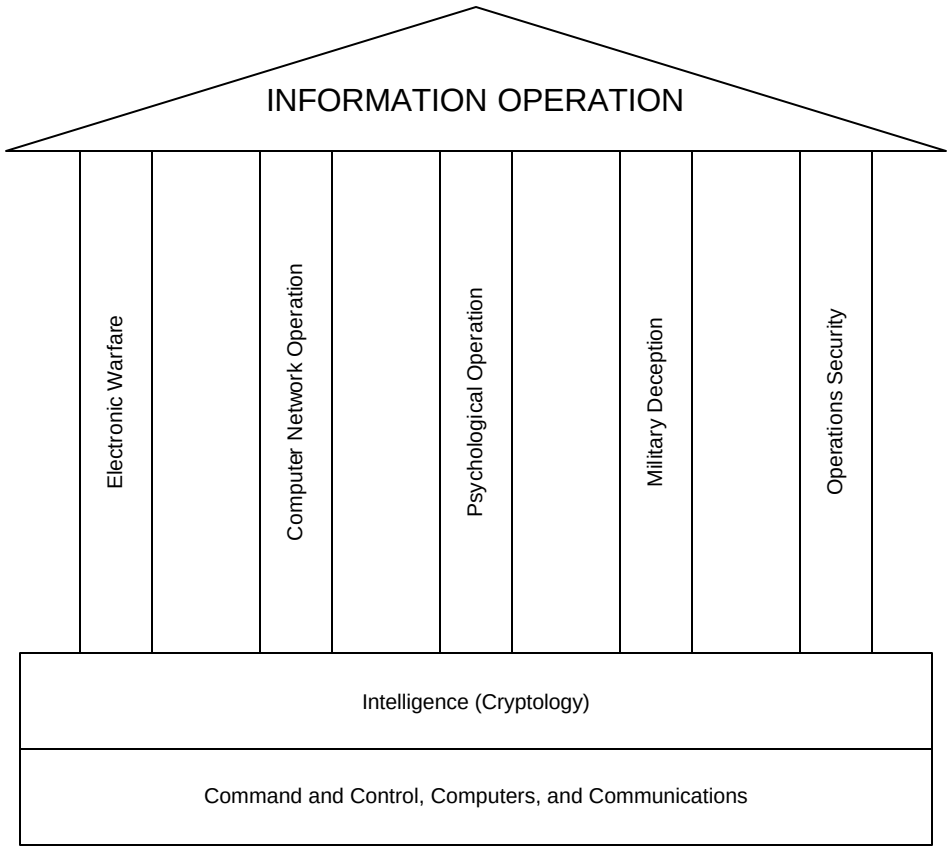


Figure 1. IO Core Competencies and Foundations[7]

1. Electronic Warfare (EW)

Electronic Warfare is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.[8] The electromagnetic spectrum is the medium through which information can be collected and disseminated. To affect the EM spectrum is to affect the information traveling across it. Therefore, EW affects information or information systems through its action on the EM spectrum or use of directed energy.

a. Electronic Attack (EA)

Electronic Attack involves actions taken to attack the adversary with the intent of degrading, neutralizing, or destroying adversary combat capability to prevent or reduce an adversary's effective use of the electromagnetic spectrum.[9]

b. Electronic Protect (EP)

Electronic Protect involves such actions as self protection jamming and emission control taken to protect friendly use of the electromagnetic spectrum by minimizing the effects from friendly or adversary employment of EW that degrade, neutralize, or destroy friendly combat capability.[10]

c. Electronic Warfare Support (ES)

Electronic Warfare Support contributes to the situational awareness by detecting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy for the purpose of immediate threat recognition.[11] ES further enhances IW by populating EW databases and providing baselines of adversary electromagnetic environment.

2. Computer Network Operation (CNO)

From *DODD 3600.1* and *AFDD 2-5*, Computer Network Operations involves action taken to affect or exploit adversary computer systems, networks, and data while defending one's own computer systems, networks and data. As an increasing amount of information needed to conduct warfare resides, in the form of data, on adversary and friendly computer systems and networks, Computer Network Operation plays an increasingly important role as a core competency in Information Warfare.

a. Computer Network Attack (CNA)

Computer Network Attack involves actions to gain access to a computer or computer network for the purpose of attacking the data, the processes, or the hardware. This may involve the use of Denial of Service (DOS) attacks, malicious code implantation, data modification, and data fabrication.

b. Computer Network Defense (CND)

Computer Network Defense involves actions taken to protect one's own computer and computer network from attack and exploitation by the adversary.

c. Computer Network Exploitation (CNE)

Computer Network Exploitation involves actions taken to exploit an adversary's computer and computer network. The exploitation takes the form of remote digital surveillance, system probing, data acquisition and ex-filtration, and gaining access for future exploitation or attack.

3. Psychological Operations (PSYOP)

Psychological Operations involve actions taken to convey a selected message to a target audience, in the target audience's native language, to induce a behavior

that supports friendly objectives.[12] In the first Gulf War, the US military effectively utilized PSYOP. The leaflet campaign in conjunction with synchronized B-52 strikes induced surrender amongst the Iraqi troops. Eventually, the leaflets had sufficient credibility to cause the Iraqi troops to abandon their position without actual strikes.

4. Military Deception (MILDEC)

Military Deception involves actions taken to convey a selected perception to a target's intelligence collection and dissemination assets for the purpose of causing adversary commanders to form inaccurate impressions about friendly force capabilities and intentions.[13] Using the example presented in the PSYOP section above, the MILDEC operation in the first Gulf War convinced the Iraqi troops that an amphibious assault was imminent at Kuwait. The displays of amphibious assault exercises off of Saudi Arabian and the demonstrations of the coast of Kuwait on the night of the actual attack into Iraq, influenced the adversary commanders to misallocate their forces to our benefit.

5. Operations Security (OPSEC)

From Joint Publication 3-54, Operations Security involves actions taken to protect or hide friendly unclassified and observable indicators from adversary intelligence collection efforts. The purpose of OPSEC is to prevent adversary intelligence from discerning friendly critical information, such as capabilities and intentions. A historical example of OPSEC in practice goes back to the Vietnam era. B-52's flew bombing missions over North Vietnam to virtually no effect. The adversary seem to figure out the times and targets of these bombing missions. Apparently, the targets were abandoned by the time they

were serviced by the B-52's. A team was assigned to determine where the compromises had occurred. It was found that all B-52 crews filed international flight plans. The adversary intelligence agents were able to gain access and analyze these flight plans. Based on this gathered information, the adversary was able to determine the target of that particular mission and the time over the target. The team recommended that all B-52 crews file the same flight plan and use the same entrance corridors to Vietnam airspace. The procedural change increased the effectiveness of each subsequent bombing mission.

6. Supporting or Foundational Competencies

As studied in *Joint Publication 3-13*, Supporting Competencies are elements through which their action will have a supporting role to the effects of the five core competencies. These competencies are Physical Destruction, Special Information Operations (also known as Special Technical Operations), Public Affairs, Civil Affairs, Intelligence supported by Cryptology, and C4 (Command and Control, Computers and Communications). Though this list is not all-inclusive, it does cover the primary recognized supporting competencies.

Physical Destruction involves actions taken to physically destroy or damage a specified target in support of the objectives. From the *Joint IO Planning Handbook*, this may involve the use of munitions or Special Forces' direct actions.

Special Information Operations involves the use of classified programs to achieve a specific effect on a target.

Public Affairs involves informing and educating the US public audience and international community on US operations and activities. This is achieved by providing selected factual information to the media and public with the intent on informing and educating.

Civil Affairs involves actions taken to reconstitute the native infrastructure of an operational area. Typically, the activities associated with Civil Affairs are the reconstruction of the infrastructure, economy, and basic services. This also includes humanitarian efforts to assist the local populace.

Intelligence, supported by Cryptology, is part of the foundation on which the five core competencies rest. Intelligence collects and provides the information necessary to conduct IW planning, targeting, and mission assessment.

C4 is the other part of the foundation on which the five core competencies rest. C4 provides the primary conduit through which all planning and execution must be coordinated and conducted.

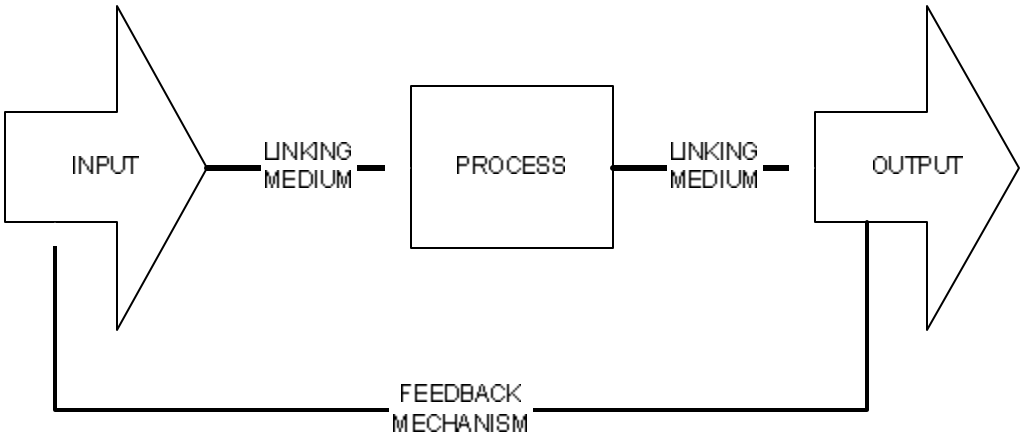
7. Related Competencies

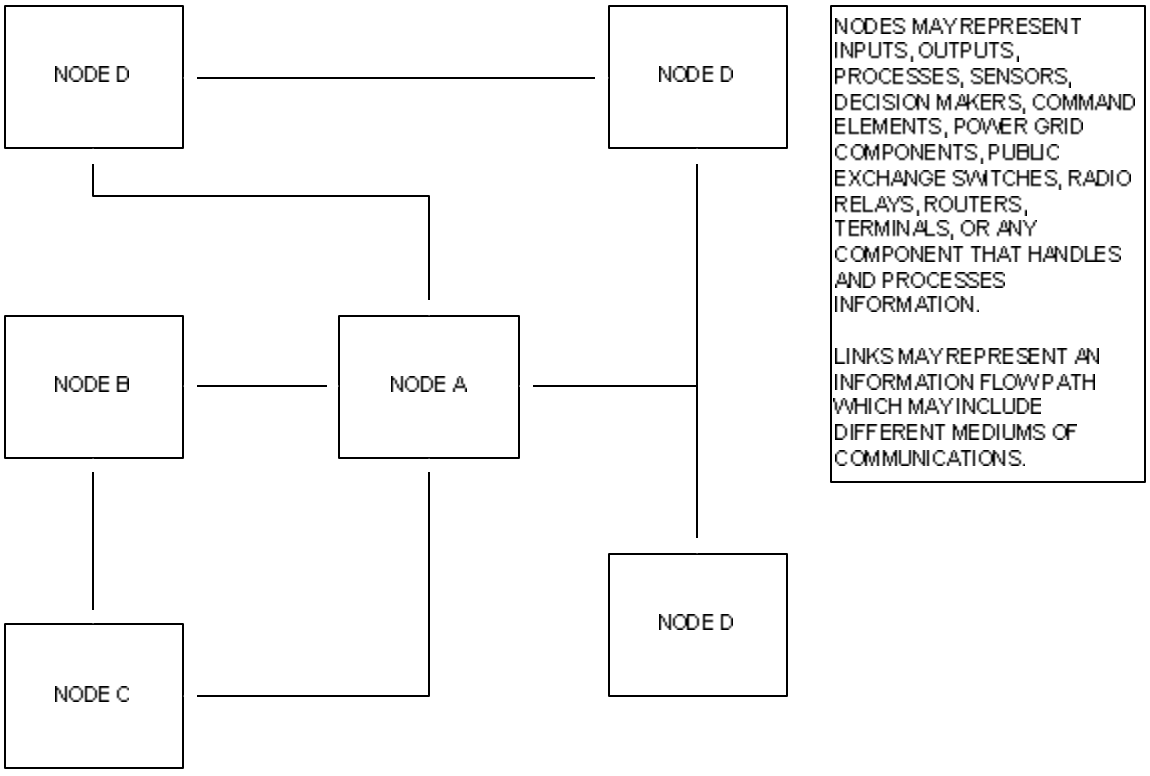
A controversial related competency is IW/IO Law and resides within the Inspector Generals/Judge Advocate Generals Community. The primary difficulty in this area is precedence. The new paradigms and technologies have brought forth new legal problems and ramifications. Rules of Engagement define how a conflict will be conducted and the legal support for those engagements. Legal interpretation by the legal community will have a tremendous impact as to how we will be able to conduct IO.

B. INFORMATION WARFARE TARGET SETS

Targets, as traditionally defined in *Joint Publication 3-60*, have been used to identify a geographical area, a complex, an installation, equipment or personnel to be serviced by conventional weaponry in support of the commander's objectives. Traditional IO targets have always been personnel, specifically the adversary decision makers, adversary commanders, troops, and the adversary populace. These targets were serviced by OPSEC, MILDEC, PSYOP, and Physical Destruction (with the emphasis placed on destruction). OPSEC targets are defined as adversary intelligence collection, which include observers and spies. MILDEC targets are defined as the adversary decision makers and commanders. PSYOP targets are defined as the adversary decision makers, commanders, troops, and populace. Since World War II and the advent of radar technology, EW has been a counter to radar. EW targets being defined as primarily radars and limited radio communications links.

With the realization of Information Operations, information and information systems are now considered targets. The scope of IW targets has expanded beyond traditional targets as defined by the Joint Targeting Process. IW targets can now be described by using a generic system model (see Figure 2) or a links and nodes model (see Figure 3). Any component in those models is a viable target provided they are accessible and vulnerable to an IW weapon or tool.


INPUT
LINKING MEDIUM
PROCESS
LINKING MEDIUM
OUTPUT
FEEDBACK MECHANISM


NODE D
NODE D
NODE B
NODE A
NODE D
NODE C
NODES MAY REPRESENT INPUTS, OUTPUTS, PROCESSES, SENSORS, DECISION MAKERS, COMMAND ELEMENTS, POWER GRID COMPONENTS, PUBLIC EXCHANGE SWITCHES, RADIO RELAYS, ROUTERS, TERMINALS, OR ANY COMPONENT THAT HANDLES AND PROCESSES INFORMATION.
LINKS MAY REPRESENT AN INFORMATION FLOW PATH WHICH MAY INCLUDE DIFFERENT MEDIUMS OF COMMUNICATIONS.

are hardware, software, wetware, and information.[15] We will examine these new classifications and how they apply to the targets of the core competencies. Though the targets mentioned here may not seem valid, their validity in the next section, IW Tools and Weapons Systems.

1. Hardware

Hardware is defined in the *Joint IO Planning Handbook* as a physical target, specifically equipment, facilities, support systems, and information systems. OPSEC's target sets within the hardware category are primarily the equipment or systems used by the adversary for intelligence collection and surveillance. This equipment can be as innocuous as a camera or as sophisticated as dedicated reconnaissance vehicles and satellites. MILDEC's target sets within the hardware category are similar to OPSEC's; though the objective is to deceive/mislead vice deny critical information. EW's target sets within the hardware category are subcategorized into radars, communications, and electronics. Radars have been the classical targets of EW. Communications have now become a more viable target. The HF through EHF frequencies are now vulnerable to EW effects. This means that radio communications (including wireless devices), microwave links, satellite uplink and downlinks are all potentially vulnerable. Electronics is the catch-all category. This category includes any device with electronic circuitry or processing chip not included in the previous subcategories. CNO's target sets within the hardware category are any computer or computer networking equipment.

2. Software

Software is defined in the *Joint IO Planning Handbook* as the data or program instruction needed by a device in

order to operate. EW's target set within the software category is the data integrity. CNO's target sets within the software category are the data integrity and data authenticity.

3. Wetware

Wetware is defined in the *Joint IO Planning Handbook* as the people and the minds of those people. OPSEC's target sets within the wetware category are intelligence analysts and the decision makers. MILDEC's target sets are the same as for OPSEC. PSYOP' target sets within the wetware category are decision makers, governments, organizations, groups, troops, and the general populace. EW's target sets include military and civilian personnel for the purpose of non-lethal engagement of potentially hostile personnel. CNO's target set is the computer operator.

4. Information

As presented in *Information Warfare and Security*, information is defined as data interpreted within a specified context to give meaning to the data. OPSEC's target set is the adversary intelligence requirements, specifically friendly critical information. MILDEC's target set is the adversary's preconceived perception of friendly capabilities and intentions. PSYOP' target set is the presentation of information content and context. EW's target set within the information category is the integrity of the information. CNO's target sets are content, integrity, and authenticity.

C. INFORMATION WARFARE TOOLS AND WEAPON SYSTEMS

The progress of technology has not only brought forth the broadening scope of IW targets, but has also ushered in

new weapons and tools to affect those targets. We will examine the traditional weapons of the five competencies of Information Warfare. We will also examine the new weapons available to Information Warfare planner through current technologies.

1. OPSEC

From *Joint Publication 3-54*, traditional OPSEC tools are the OPSEC Survey, awareness training, print media, and procedural or organizational changes. The OPSEC Survey is a tool used by OPSEC practitioners to determine OPSEC status of an organization or operation. This survey is completed by the members of an organization or operation. It seeks to determine where observable, identifiable indicators, which may expose critical information, exist. Once these indicators have been identified, a risk analysis is performed to examine the cost of countermeasures versus the benefit provided by those countermeasures. When countermeasures are viable, they are implemented. These countermeasures are typically in the form of procedural or organizational changes. Awareness training is conducted to maintain the OPSEC readiness of an organization or operation. Print media in the form of security posters, flyers, and organizational newsletters. With new technologies, the scope of the media has expanded to electronic communications, (email, screensavers, etc.). Also posters and flyers provided for awareness.

2. MILDEC

From *Joint Publication 3-58*, traditional MILDEC tools can be classified into three different categories; physical, technical, and administrative. Physical tools include displays, feints, demonstrations, and ruses. Physical tools rely on actual maneuvers or actions by

friendly forces. Technical tools include camouflage, shapes, radar reflectors, decoys, false communications networks, and false radar emissions. Administrative tools include a staged compromise or loss of classified documents, as described in WWII allied operation “Mincemeat” and discussed in the book “The Man Who Never Was” by Ewen Montagu. With new technologies, the traditional tools of MILDEC are still applicable.

3. PSYOP

As described in *FM 33-1-1*, traditional PSYOP tools can be divided into two broad categories; media and delivery platforms. Media is the medium in which a PSYOP message is delivered. Media can be further subcategorized into audiovisual, visual, audio, and personal. Audiovisual media can be characterized as media delivery both sight and sound. Examples of audiovisual media are television and motion pictures. Visual media are media which delivers its message by sight only. Examples of this are leaflets, pamphlets, posters, books, and art. Audio media delivers its message through sound. Examples are radio and loudspeakers. Personal media is face-to-face communications with the intended audience. Delivery platforms are equipment or vehicles which utilize one category of media to deliver the PSYOP message. Delivery platforms and the associated media are listed below in Table 1. New PSYOP tools and weapons available are Transportable AM-FM Radio Broadcasting Station (TARBS) and Hypersonics/Audio Spotlight. TARBS is a deployable broadcast station, which can be placed on ships to serve as an afloat or ashore broadcasting station. Hypersonics is a recent development in speaker technology. It employs the use of ultrasonic waves modulated by audible sound waves to transmit sound.

When the ultrasound collides with an object, the distortion caused by the impact demodulates the audible sound waves. The localize demodulation creates sound in the immediate area of the object. The scope of this technology as it pertains to PSYOP is great. Now, a PSYOP message can be delivered with pinpoint accuracy at a target. Audio Spotlight is the consumer product line utilizing this technology.

4. EW

From *Joint Publication 3-51*, traditional EW tools and weapons are jammers and decoys. EW jammers transmit electronic noise on the frequency of the radar being targeted. Communications jammers transmit noise on communications frequencies (HF-VHF-UHF). Traditional decoys are chaff, radar reflectors, and flares. Chaff is a fine strip of radar reflective material cut to a length optimized for certain radar frequencies. Radar reflectors are expendable decoys, which attempt to reflect a larger amount of radar energy than the platform it is protecting. Flares are decoys designed to defeat infrared systems.

As described in *Electronic Warfare in the Information Age*, new technology has brought new tools, techniques, and weapons. EW jammers are no longer limited to noise jamming. Recent EW jammers are capable of Deceptive Electronic Countermeasures (DECM). DECM is a technique to receive radar energy, manipulate the waveform, and transmit a jamming signal optimized to defeat that radar system. Communications jammers have also been updated to be able to transmit specific waveforms.

Delivery Platform	Media Utilized
Portable Transmitters	Audio: AM-FM Radio Audiovisual: Television
Ground Vehicles	Audio: Loudspeakers, AM-FM Radio Audiovisual: Television
Helicopters	Audio: Loudspeakers, AM-FM Radio Audiovisual: Television Visual: Leaflets
Aircraft (Temporary Set Up)	Audio: AM-FM Radio Audiovisual: Television Visual: Leaflets
M129 Leaflet Bombs	Visual: Leaflets
Leaflet Boxes	Visual: Leaflets (dropped by Helicopter or Aircraft)
EC-130E Commando Solo	Audio: AM-FM Radio Audiovisual: Television
Troops	Personal: Civil Affairs Visual: Leaflets, Pamphlets
Various Product Production System	All
Note: Detailed descriptions available in FM-33-1-1.	

Table 1. PSYOP Delivery Platforms (from FM-33-1-1)

Also described in Electronic Warfare in the Information Age, in addition to traditional decoys, electronic decoys are now available. These electronic decoys transmit electronic signature of the platform they are protecting. Traditional flares have been upgraded and

augmented. Flares are now capable of specific frequencies of infrared to counter filters implemented by offensive infrared systems. There are now active infrared defense systems to augment the flares.

One of the newest developments in EW is High Powered Microwave devices (HPMs) or High Energy Radio Frequency devices (HERFs). HPMs/HERFs generate high-powered emissions to destroy electronic circuitry. The E-Bomb or more accurately named conventional electromagnetic pulse bomb generates a short duration high-energy pulse, similar to the EMP effects from a high altitude nuclear detonation. HPMs have also been used to target personnel. These HPMs cause intolerable pain to the target in order to persuade the target to take other less offensive actions.

New pseudo-EW weapons, which also target personnel, are the sonic weapons. Sonic weapons are potentially non-lethal weapons, which can have similar effects as the HPMs, incapacitate their target personnel. Hypersonics, mentioned earlier in the PSYOP section, is a potential weapon against troop. With hypersonics, friendly forces can shoot a pinpoint beam of sound in excess of 150 yards. The sound heard at the target location can be set to 145 dB, which is 50 times the threshold of pain for humans. Though sonic weapons are not technically EW weapons, we include them here because of their similarity.

5. CNO

CNO has no historical weapons due to its relative recent introduction (last 5-10 years). We will examine CNO tools and weapons in a logical sequence. First, we will look at tools for CNE. CNE will lead us into CNA tools. We will forego CND tools, as our focus is to target

offensively. Our primer for this study into CNO and its elements will be Hacking Exposed, Third Edition, 2002. One caveat to this is we will assume all activities will be conducted online. A second caveat is that all examples discussed here are widely available, non-military tools. This is to preserve the classification and distribution of this study.

CNE tools have varying complexity and intrusiveness. The least intrusive is an internet search engine, such as Google, WebCrawler, Whois, etc. The next tools are domain register search engines such as Sam Spade. These tools provide greater detail of the intended target's computer systems and networks. The next step is scanning tools. Scanning tools allow us to map the target's computer network. These tools include Nmap and Superscan. Next, we need to determine the specifics of individual components of the network. The enumeration tools are DumpSec, NAT10, and Legion. We have now reached the juxtaposition between CNE and CNA. This border is defined by intent. If the intention is to only exploit, then you remain in CNE. However, if the intention is to alter data, deny access, change configuration, or plant destructive code, then from *Joint Publication 3-13*, you have crossed into CNA. Additional tools to gain and elevate access onto a network are TCPDump, L0phtcrack, TFTP, NetCat, etc.

CNA tools can be divided into five general categories; data altering, cleaning, backdoors, denial of service, and malicious codes. Data altering tools include text editors, file editors, file command functions, and address resolution protocol (ARP) table protocol manipulators. Cleaning tools remove any record of your activity on the

network. Some tools are rootkits (Back Orifice and SubSeven), text editors, file editors, registry editors, and file command functions. Backdoor tools create alternate access to the system or network. Denials of Service (DOS) tools deny service to the targeted system’s users. Some of these tools are Synk4, Ping of Death, Smurf Attack, Supernuke.exe. Malicious code tools are tools that create malicious code or the code itself. The codes are classified as worms, virus, Trojan horses, logic bombs, etc. A more extensive list of tools and techniques can be found in Hackers Exposed, Third Edition, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TARGETING

A. TRADITIONAL TARGETING

Traditional targeting processes and methodologies are best described in *Joint Publication 3-60* and *FM 90-36 TARGETING: Joint Targeting Process and Procedures for Targeting Time-Critical Targets* developed by the Air Land Sea Application Center. This document is the primary source for further exploration into the Joint Targeting Process. In order to understand Joint Targeting, we must first define a target. As stated previously, a target can be a geographical area, a complex, an installation, equipment or personnel. The Joint Targeting Process exists because of the need to deconflict targeting operations, prevent duplication of effort, and reduce the potential for fratricide and collateral damage in a dynamic battlespace environment. The Joint Targeting Process must ensure the following:

1) Compliance with the Commander’s guidance and objectives.

2) Coordination, deconfliction, and synchronization of all targeting efforts.

3) Prevent fratricide.

4) Minimize collateral damage.

5) Minimize duplication of effort.

6) Control tasking for mutually accessible targets.

7) Provide expeditious combat assessments.

8) Provide a common perspective for all of the targeting effort.

The primary goals of the Joint Targeting Process are to ensure the most efficient use of joint force assets and to capitalize on synergistic effects. The Joint Targeting Process is a set of function, steps, and actions required to conduct Joint Targeting. The Joint Targeting Process is a six phase cyclical process shown in Figure 4.

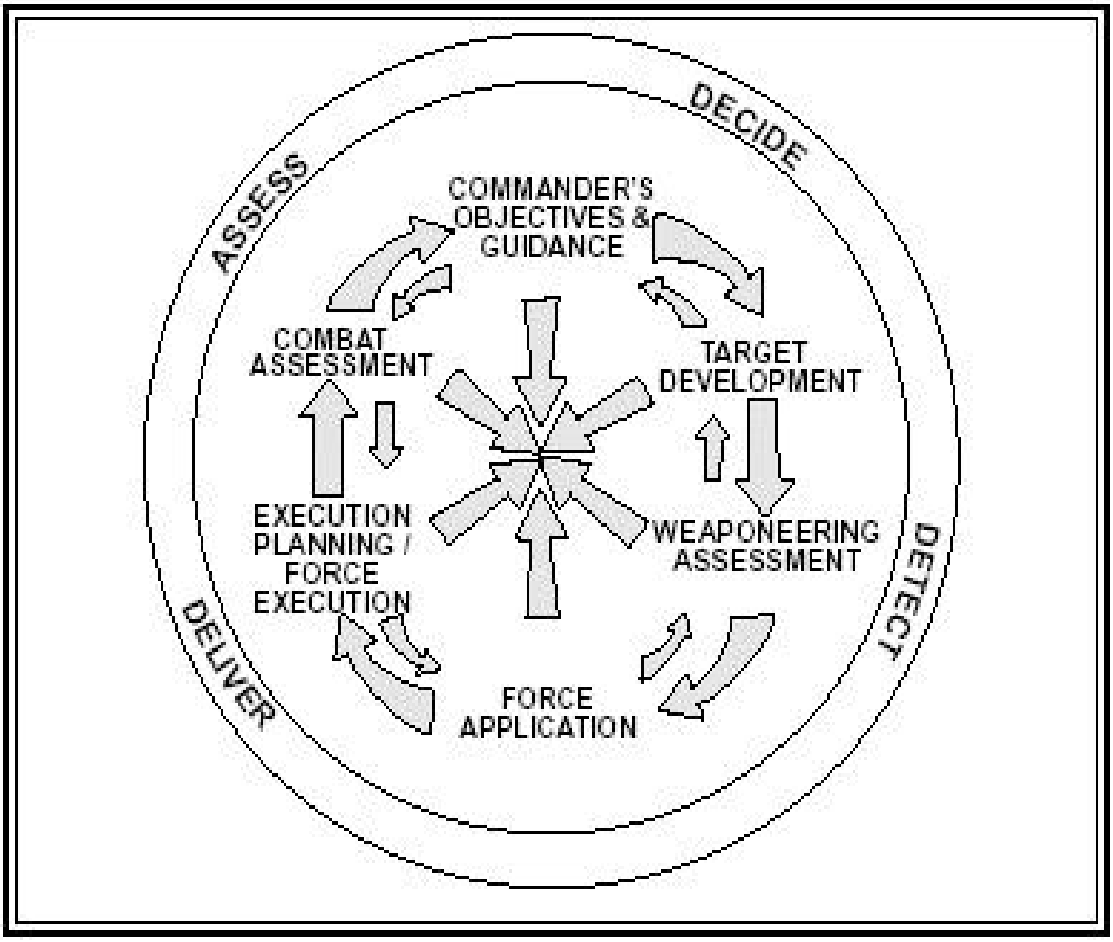


Figure 4. The Joint Targeting Process[16]

Also shown in Figure 4 is the Army and Marine Corps four-step targeting methodology, Decide-Detect-Deliver-Assess. This joint targeting process determines the employment of military force to achieve a desired objective and is driven by the commander’s objectives and guidance.

1. Commander’s Objectives, Guidance, and Intent

From *FM 90-36* and the *Joint IO Planning Handboo*k, the commander’s objectives are his/her desired position, outcome, or purpose of the operation. The commander’s guidance is the framework for employing theater assets to achieve the objective. The commander’s intent is his/her plan to achieve the objective. Good objectives and guidance have 3 characteristics. They are clear, measurable, and attainable. They also include an articulation of damage levels, desired states, and period of operation.

2. Target Development

From *Joint Publication 3-60* and *FM 90-36*, Target Development Phase is the systematic evaluation of potential target systems, individual targets, and the element of each target. There are three basic targeting criteria: criticality, accessibility, and vulnerability. Criticality is the relative importance to attaining the commander’s objective and/or the relative importance as the target relates to other systems. Accessibility is ease with which friendly forces or munitions are able to physically get to the target. Vulnerability is the target’s vulnerability to the effects of the munitions or forces used against it.

3. Weaponeering Assessment

From *FM 90-36*, Weaponeering Assessment Phase provides various force application options for each target based on the desired effect. This assessment is based on an analysis of the target’s characteristics and vulnerabilities. Weaponeering assessment determines the quantity, type, and mix of lethal and non-lethal options required to achieve the desired effect. This phase attempts to optimize target-weapon-effect matching.

4. Force Application

From *FM 90-36*, Force application phase combines the results of the weaponeering assessment with the available force to deliver them. This phase seeks to optimize force employment to minimize effort. The key products from the force application phase are the Master Air Attack Plan/Air Tasking Orders and the Master Ground Attack Plan/Attack Guidance Matrix.

5. Execution Planning and Force Execution

From *FM 90-36*, Execution Planning involves the conduct of mission planning for each individual element and preparations for engagements. This portion of the phase involves scheduling, mission assignments, routes, and tactics.

Force Execution involves executing the planned missions and monitoring the operation. This is typically a component commander function and includes real-time recommendation, redirection of forces, re-attack assignments.

6. Combat Assessment

From *FM 90-36*, Combat assessment determines the overall effectiveness of force employment and whether the commander’s objectives are being met. This is primarily an intelligence function and includes: battle damage assessment (BDA), munitions effectiveness assessment (MEA), bomb hit assessment (BHA), and re-attack recommendation.

These methods are still based on the old paradigms of using conventional weaponry.

B. INFORMATION WARFARE TARGETING

Information Warfare targeting is based on the current Joint Targeting Process. With IW targeting and planning, this study has discovered that the traditional timelines used by the Joint Targeting process must be reevaluated. This study will also examine IW targeting in the context of the traditional targeting process.

1. Commander's Objectives, Guidance, and Intent

Based on *Joint Publication 3-60*, the commander's objective, guidance, and intent apply the same as in the traditional targeting process. However, it must now be interpreted by the IW staff into IW objectives and tasks. After coming to a full understanding of the commander's objectives, guidance, and intent, the IW staff must fully understand the adversary. The key is to understand the adversary's perspective. Understanding the adversary's perspective will lead to the IO objectives and desired effects as described in the Joint IO Planning Handbook.

2. Target Development

Based on the Joint IO Planning Handbook, in IW target development, we must conduct a systematic evaluation of the adversary's information and information systems. This evaluation must take into account the four IW target categories hardware, software, wetware, and information. We can use the links and nodes relational model to evaluate these targets. As presented in the Joint IO Planning Handbook, we must understand the significance of the information to the adversary, how that information will be used, the information systems that process the information, the flow of that information through the adversary systems, and vulnerabilities associated with the entire system. Once

we understand the relationship between the various nodes and the links, which carry the information, we can identify targets within the system. From the identified targets, we select targets and desired effects, which will contribute to achieving the IO objectives.

3. Capability Analysis (Weaponeering Assessment)

From the *Joint IO Planning Handbook* and *Joint Publication 3-60*, capability analysis[17], which is the equivalent to weaponeering assessment, examines the targets selected in the target development phase and identify which of the IO competencies (core and supporting) will be most effective in achieving the desired effect. This may involve the application of multiple competencies and other warfare areas. From the identified competencies, we will select the tools or weapons that will best achieve the desired effect, which can be lethal or non-lethal. The final product being a weapon/tool-target-effect matching. In addition, clear measures of effectiveness (MOEs) must be established in order to determine whether the objectives have been achieved, as stated in the Joint IO Planning Handbook.

4. Force Application

In IW force application, we take the results of the capability analysis and assign available forces for execution. Like traditional force application, IW force application seeks to optimize force employment and minimize effort. However, from *Joint Publication 3-13*, what is more critical is the synchronization of effort in order to capitalize on synergistic effects. This synchronization is best described by using perception management. Using PSYOP to influence the adversary to reinforce a preconceived notion of friendly forces and MILDEC to further reinforce what the adversary is expecting to see and hear. OPSEC then

protects the real operation. The synchronization of these efforts produce an effect much greater than neither could have achieved alone. One of the best examples is the amphibious feint in the first Gulf War. PSYOP reinforced the Iraqi notion that the US Marines were legendary combat troops. Military Deception produced displays of amphibious exercises and a feint into Kuwait, while OPSEC concealed the true troop movement to the west.

5. Mission Planning and Execution

From *Joint Publication 3-60* and the *Joint IO Planning Handbook*, IW Mission Planning and Execution is the same as traditional execution planning and force execution. IW forces will conduct the detail planning and execution of the mission to deliver the weapon or tool to the adversary targets.

6. Combat Assessment

From the *Joint IO Planning Handbook*, Combat Assessment is also the same as traditional combat assessment. The criteria for success or failure are compared to the MOEs established in the capability analysis phase. Intelligence collection may require long-term analysis to determine the efficacy of IW effects. Intelligence collection may also require analysis of related or secondary system to determine the achievement of IW objectives.

C. COMPARE AND CONTRAST TARGETING CONCEPTS

In this section, we will examine the difference in traditional targeting and Information Warfare Targeting. We will study the inherent advantages and disadvantages of integrating these two processes.

The advantages of traditional targeting process when applied to IW are:

1) For list numbering, use either n. or n) but not n.).The process is standardized and familiar to all planning staffs and services. Familiarity instills confidence.

2) The process has a relatively short cycle times. Typically, it coincides with the 72 hours Air Tasking Order (ATO) generation process.

3) It is very effective with conventional targets, because it was designed around conventional weaponry.

The disadvantages of traditional targeting processes when applied to IW are:

1) Only one universally recognized target identification and reference system. This system is designed specifically for conventional targets.

2) Procedures for the Joint Target Coordination Board (JTCB) and the Guidance, Apportionment, and Targeting (GAT) Cell vary between theaters of operation.

3) Joint Doctrine does not explain how to perform actual targeting.

4) Current tactics, techniques, and procedures do not outline the specifics of targeting.

The advantages of a unique IW targeting process are:

1) It is designed for IW.

2) It is based on the traditional targeting process.

3) It is synchronized to capitalize on synergistic effects.

The disadvantages of a unique IW targeting process are:

1) The planning staffs and services are less familiar with IW concepts.

2) Paradigm shifts are usually met with resistance initially.

3) The timelines for planning, execution, and combat assessment vary among the IW competencies. Some competencies require long lead times for execution and combat assessment.

The advantages of integrating the two processes are:

1) It will permit other warfare areas to coordinate with IW efforts to maximize the advantages of effects based operation through synchronization of the effort.

2) It will allow for synergistic effect between IW and the other warfare areas. It will allow IW to act as a force multiplier for the other warfare areas and it allows the other warfare areas to lend credence to the IW efforts.

The disadvantages of integrating the two processes are:

1) The timeline variation in IW planning, execution, and combat assessment will add complexity to the targeting process. IW, as a whole, cannot abide by the ATO generation timeline.

2) All the disadvantages, to varying degrees, listed for the traditional targeting process and for the IW targeting process.

The payoff for overcoming these disadvantages is the optimization of force employment, “munitions” expenditure,

and effects to achieve the objectives. Other payoffs are the alleviation of risk to forces, shortening the duration of the conflict, and minimizing the cost of the conflict. The payoff is best stated in the following:

> Properly executed, IO could have halved the length of the campaign…
>
> Admiral James O. Ellis, United States Navy
> Commander-in-Chief, US Naval Forces Europe
> Commander, Allied Forces Southern Europe
> Commander, Joint Task Force NOBIL ANVIL
> During Operation ALLIED FORCE

IV. INFORMATION WARFARE TARGETING COURSE DEVELOPMENT

A. COURSE RESEARCH

The research conducted for this document was also used in the creation of the Naval Postgraduate School's IW Targeting Course, IW3920. All of the reference documents listed in the reference section of this document were used in the preparation of the course. The focus of the course research was from a joint combatant command perspective. A course review was done on IW courses and IW targeting courses offered by the individual services and the Joint Forces Staff College. These courses (shown in Table 2) were examined for their insight and guidance on the creation of this course.

Organization	Course Examined
Joint Forces Staff College	Joint Information Warfare Staff and Operations Course
Air Force Special Operations School	Special Operations Forces Information Operations Planner Course
Air Force Information Warfare Center	IW Applications Course
Fleet Information Warfare Center	Naval Information Warfare Staff and Operations Course
1st IO Command (Formerly known as LIWA)	Information Operations Capabilities, Applications, and Planning

Table 2. Courses Examined for Research

B. COURSE DEVELOPMENT

We developed a course that provides the foundations of the target planning processes as it applies to Information Warfare. The previous course was heavily focused on the technical aspects of targeting. The course that we developed replaces the previous course with a more rounded treatment of IW. Each core competency of Information Warfare is studied and targeting concepts are applied.

The idea is to convey to the students the art of information warfare targeting through lecture, course work, practical examples, and hands-on analysis. One difficulty with the course development was to ensure the proper scope of material could be covered without overlapping other coursework. This problem was due to the pre-requisite class of IW3101 and the follow-on class of IO4300. The solution was to tread carefully between the two and minimize the overlap of the material. In IW3101, the students learned the fundamental theories behind IW. In IO4300, the students learned to incorporate those theories into operational planning. The solution was to focus on the practical targeting aspects of IW. The goal is to educate students on the art and science of IW targeting and the potential applications of IW tools for a desired effect.

To achieve this goal, we used an approach involving the idea of using the links and nodes relationship model, also known as nodal analysis. Targeting the links or the nodes was the premise behind this course development. The idea is to teach the student to place a target or system in a framework that will facilitate evaluation of that target or system. We covered the intelligence requirement to analyze the links and nodes targeting model for each IW

core competency. Finally, we covered the application of weapons and tools for each competency to show the effects that can be achieved. We took the five core competencies and allowed three days of lecture for each competency. The first day covers the links and nodes relationship for that particular competency and the analysis required for target selection. The second day focuses on the intelligence requirements to analyze the relational model and the sources of this intelligence. The third day examines the weapons and tools needed to achieve the desired effects on the selected target.

As most of the students had little or no exposure on planning or targeting, it was necessary to expose them to the Joint Operations Planning and Execution System (JOPES) and the Joint Targeting Cycle. It was also necessary to cover the joint targeting process in detail.

Perception Management is an overarching term for the collection of PSYOP, MILDEC, and OPSEC. After each of these competencies was covered, the synergistic effect of these three competencies working in concert was illustrated.

Supporting and related competencies are vital to the success of IW. Additional lectures were included to show the effects of these competencies on the core competencies.

Two lectures were required to show how all of these competencies work synergistically.

Lab time was used to provide guest speakers, who are subject matter experts, to discuss targeting in their particular IW competency (see Table 3). Lab time was also designed to give the students hands-on experience with

IW/IO planning tools available to staff planners, such as IO Navigator (ION) and Information Warfare Planning Capability (IWPC).

The efficacy of the material was measured by weekly quizzes, a research paper, and a final class project. Quizzes consisted of multiple choice, fill-in-the-blank, and short essay questions. The research paper provided the students an opportunity to delve into a specific IW targeting topic. The final class project provides the best measure whether the material was being sufficiently understood by the students.

C. COURSE PLAN

The material derived from this research and course development effort was used to create an 11-week graduate level course. We also adapted this course to electronic media to facilitate distance learning by mid-grade officers unable to physically attend due to operational commitments. The course plan shown on Table 3 displays the schedule developed for this course. A grading policy was established with the following breakdown: Final Class Project – 40%, Quizzes – 30%, Research Paper – 20%, and Class Participation – 10%. This policy was developed to give more weight to the final class project than the other aspects of the class.

Week	Lectures			Labs/Speakers
1	Introduction Policy & Grading	IW3101 Review	JOPES Planning Process	Lab Introduction Account Requests
2	Targeting Process	Targeting Process	Targeting Process	IO Navigator Lab I IOPT
3	Computer Network Operations Targets Links & Nodes	Computer Network Operations Intelligence Requirements	Computer Network Operations Applied IW	Speaker: CNO Speaker
4	TAD Collective Reading Assignments	TAD Collective Reading Assignments	TAD Collective Reading Assignments	TAD Reading Assignment Papers Due following Monday
5	Electronic Warfare Targets Links & Nodes	Electronic Warfare Intelligence Requirements	Electronic Warfare Applied IW	Speaker: EW Targeting Capt Shawn Cunningham
6	PSYOP Targets Links & Nodes	PSYOP Intelligence Requirements	PSYOP Applied IW	Speaker: 4th POG MAJ Hugh Sutherland
7	Deception Targets Links & Nodes	Deception Intelligence Requirements	Deception Applied IW	Speaker: Col(Ret) Hy Rothstein
8	OPSEC Targets Links & Nodes	OPSEC Intelligence Requirements	OPSEC Applied IW	Speaker: Ray Semko IOSS
9	Memorial Day NO CLASS Scheduled	Perception Management Synergism	Supporting Competencies	IO Navigator Lab II
10	Related Competencies	IW Synergism	IW Synergism	Free Lab Time for Projects
11	Wrap-Up Free Discussion	Student Presentations	Student Presentations	

Table 3. IW3920 Course Schedule for Spring 2003

D. COURSE PRESENTATION

This course was presented to the current Information Warfare Curriculum students to evaluate the efficacy of this instructional program and its material. Course is

designed to be a three lecture hours and two lab hours per week. The course was presented to the class in accordance with the course plan shown in Table 3.

The Blackboard learning support system was used for class administration. Blackboard is a tool available at many graduate institutions. This tool provides a forum for the students to retrieve course documents (syllabus, slide presentation, homework assignments, etc.), take exams, examine their grades, submit their work, and communicate with classmates and the instructor. This tool is ideal for distance learning application.

One aspect of grading was the weekly quizzes, which were administered via Blackboard. The weekly quizzes were designed to gauge the progress of the students. A second aspect of grading was the research paper. The research paper was assigned during the fourth week to allow the students to study a facet of IW that was of interest to him or her. The final project was the culmination of the entire course and allowed the students to apply what they have learned. For the final class project, the students selected a country or organization of interest to them, analyzed that country or organization, selected targets, determined the desired effects, and applied IW against those targets. Then, the students briefed their classmates on their project. The intent was for the students to select an objective and analyze the problem, meet the chosen objective, and present their ideas. This final project illustrated that the students understood the material and that they had learned innovative thinking about the possibilities for the application of IW.

E. STUDENT FEEDBACK AND RECOMMENDATIONS

The class consisted of 12 students; six USN Officers, three USMC Officers, and three USA Officers. Nine students were in the IW Curriculum and three were in the ISO Curriculum. Overall impression from the students was positive. The entire class thought that it was worthwhile and value-added to their understanding of IW and IW targeting. Some felt the course was similar to IW Fundamentals, IW 3101. Feedback was solicited from the students upon completion of the course.

The students provided feedback and recommendations on course material. Most students were pleased to get exposure to the JOPES planning process, as they had not seen it before. The only exception was an officer who had staff planning experience. This exception was an anomaly rather than the norm. All the students felt the study of the joint targeting process was beneficial to their understanding of targeting. The students were especially enthusiastic about the links and nodes relationship model and the framework it provided for IW targeting.

Students also provided feedback on testing and grading. Some students did not like weekly quizzes and prefer weekly papers. Most thought the quizzes were fair and covered the relevant material for those lecture periods. All of the students found the grading policy to be fair.

The students provided feedback on the final project as well. The students felt that the final class project lacked guidance. Specifically, the students commented that there was a lack of a commander’s objective and guidance. They were unsure of the content of the product they were being

asked to produce. This feedback has been used to improve the structure of the final project for future classes.

V. FINDINGS AND RECOMMENDATIONS

As presented in *The Principles of War in the Information Age,* the paradigm shift that is occurring in targeting and in military affairs is a result of the Information revolution. Conventional weaponry and destruction are no longer the only means of affecting the adversary. Recognition of IW as a warfare area is a sign of this change. IW can achieve objectives without crossing the borders of an adversary. From the *National Strategy to Secure Cyberspace,* in cyberspace, there are no borders. IW can influence the behavior of the adversary, so the objective can be achieved without having to bring conventional weapons to bear. However, IW is still an unfamiliar territory for some in the military and IW targeting is equally unfamiliar. We must integrate IW targeting with the traditional targeting process to facilitate IW's contribution to the combatant commander's effort. An IW Targeting Course can alleviate the unfamiliarity while expanding the limits on how we achieve the objective.

Improvements in targeting methodology are rooted in translating the objectives to realistic effects. These effects must then be evaluated to determine which targets can achieve those effects. These targets must now be evaluated to see all the influences working on those targets. To that end, we developed a cause-effect relational model (see Figure 5) from the links and nodes relation model described earlier. The use of this model as a framework for instructing student will aid in comprehension and can stimulate synergistic thinking.

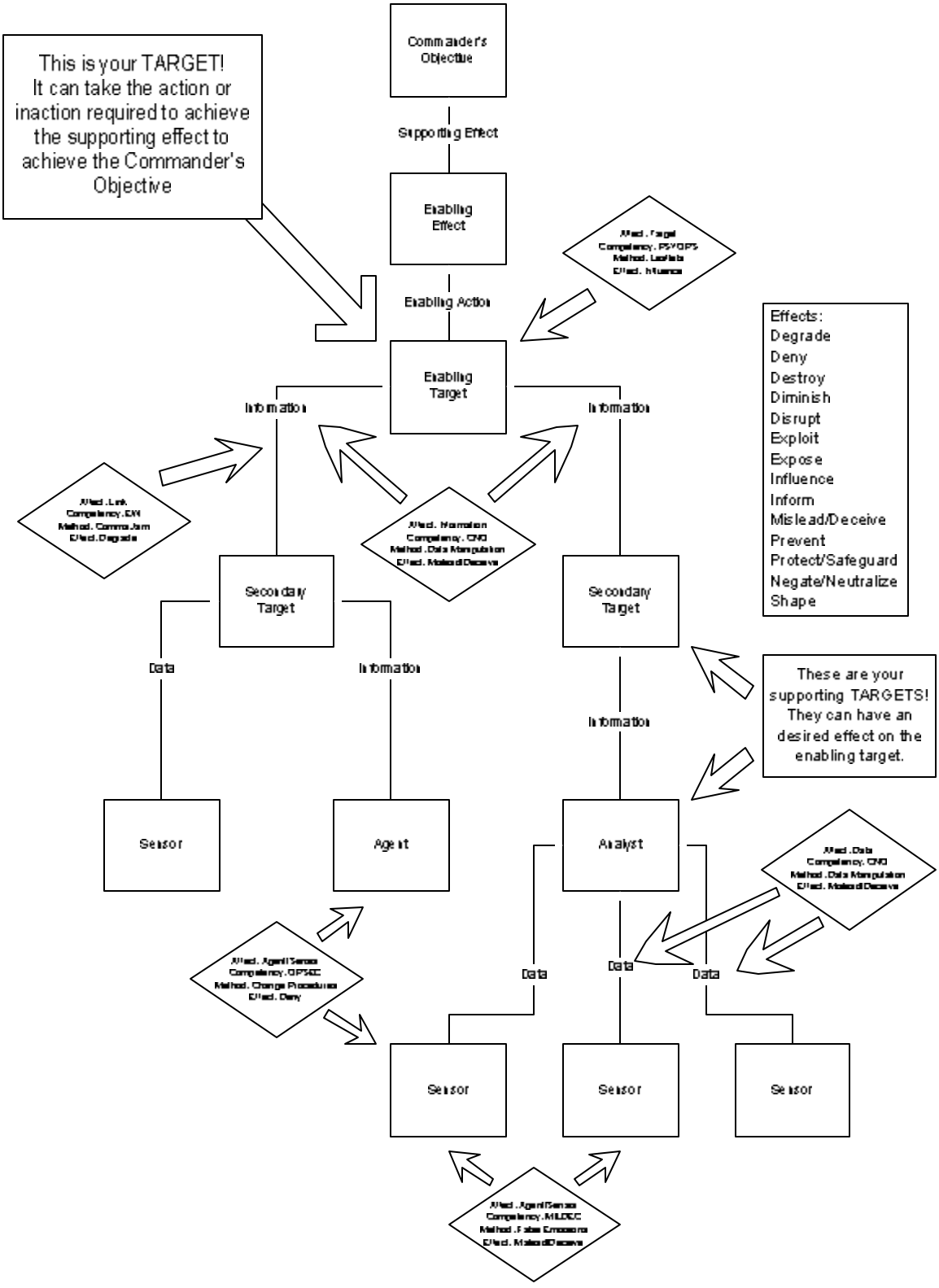


Figure 5. A Cause-Effect Nodal Model with IW affecters created by the author.

Improvements in IW targeting integration are related to the amount of time spent on the subject. A more thorough treatment of how to integrate IW targeting into traditional targeting will be provided. Adding a discussion on the synchronization matrix to the course would be beneficial.

Improvement in laboratory work and time are related to optimizing the use of student time. Additional lab work involving hands-on experience conducting targeting in support of IW in a classified environment would be most beneficial. These labs would allow the students access to intelligence material needed to conduct IW targeting. Discussions are underway with JIOC and Sandia National Laboratory to accomplish this objective.

THIS PAGE INTENTIONALLY LEFT BLANK

ENDNOTES

1 Clausewitz, Carl von, p.76

2 Sun Tzu, p.77

3 Hart, Capt Sir Basil Liddell, as quoted in JP 3-13

4 JP 3-13, p. vii

5 JP 3-13, p. I-11

6 JP 3-13, p. I-9

7 Derived from FIWC’s NIWSOC Course and JP 3-13, p. I-9

8 JP 3-13, p. II-5

9 JP 3-13, p. II-5

10 JP 3-13, p. II-5

11 JP 3-13, p. II-5

12 JP 3-13, p. II-4

13 JP 3-13, p. II-4

14 Derived from Nodal Analysis Techniques

15 As defined by the Joint Information Operations Center

16 FM 90-36, p. I-3

17 Joint Forces Staff College, p. II-6

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. 1st Information Operations Command, *Information Operations Capabilities, Applications, and Planning Course*, Fort Belvoir, Virginia, 2003.

2. Air Force Information Warfare Center, *IW Applications Course*, Lackland Air Force Base, Texas, 2002.

3. Air Force Special Operations School, *Special Operations Information Operations Planner Course*, Air Force Special Operations Command, Hurlburt Field, Florida, 2003.

4. Air Land Sea Application Center, *FM 90-36 TARGETING: Joint Targeting Process and Procedures for Targeting Time-Critical Targets*, Washington, D.C., 25 July 1997.

5. Audio Spotlight, Holosonic Research Labs [http://www.holosonics.com/technology.html],2002. February 2003.

6. Clausewitz, Carl Von, *On War*, Princeton University Press, Princeton, New Jersey, 1976.

7. Denning, Dorothy E., *Information Warfare and Security*, Addison-Wesley, Boston, Massachusetts, 1999.

8. Department of Defense, *DODD 3600.1 Information Operations*, Washington, D.C., 9 December 1996

9. Fleet Information Warfare Center, *Naval Information Warfare Staff and Operations Course*, Little Creek Naval Amphibious Base, 2003.

10. Headquarters, United States Army, *Psychological Operations Techniques and Procedures*, Washington, D.C., 5 May 1994.

11. Hypersonic Sound, American Technology Corporation [http://www.atcsd.com/tl_hss.html], 2001. March 2003.

12. Joint Chiefs of Staff, *CJCSM 3122.01 Joint Operations Planning and Execution System Volume I*, Director for Operational Plans and Joint Force Development, Washington, D.C., 14 July 2000.

13. Joint Chiefs of Staff, *CJCSI 3213.01A Joint Operations Security*, Director for Operational Plans and Joint Force Development, Washington, D.C., 1 December 1995.

14. Joint Chiefs of Staff, *User's Guide for JOPES*, Director for Operational Plans and Joint Force Development, Washington, D.C., 1 May 1995.

15. Joint Chiefs of Staff, *User's JP 3-13.1 Joint Doctrine for Command and Control Warfare*, Director for Operational Plans and Joint Force Development, Washington, D.C., 7 February 1996.

16. Joint Chiefs of Staff, *JP 3-51 Joint Doctrine for Electronic Warfare*, Director for Operational Plans and Joint Force Development, Washington, D.C., 7 April 2000.

17. Joint Chiefs of Staff, *JP 3-53 Doctrine for Joint Psychological Operations*, Director for Operational Plans and Joint Force Development, Washington, D.C., 10 July 1996.

18. Joint Chiefs of Staff, *JP 3-54 Joint Doctrine for Operations Security*, Director for Operational Plans and Joint Force Development, Washington, D.C., 24 January 1997.

19. Joint Chiefs of Staff, *JP 3-58 Joint Doctrine for Military Deception*, Director for Operational Plans and Joint Force Development, Washington, D.C., 31 May 1996.

20. Joint Chiefs of Staff, *JP 3-60 Joint Doctrine for Targeting*, Director for Operational Plans and Joint Force Development, Washington, D.C., 17 January 2002.

21. Joint Command, Control, and Information Warfare School, *Joint Information Operations Planning Handbook*, Joint Forces Staff College, Norfolk, Virginia, January 2002.

22. Joint Command, Control, and Information Warfare School, *Joint Information Warfare Staff and Operations Course*, Joint Forces Staff College, Norfolk, Virginia, 2003.

23. Joint Information Operations Center, *Information Operations Navigator (ION) Release 2.0: Startup Tutorial*, San Antonio, Texas, 15 October 2001.

24. Kopp, Carlo, *Information Warfare: 1. A Fundamental Paradigm of Infowar 2. Issues in Current Infowar*, [http://www.csse.monash.edu.au/~carlo/archive/IW/IW-2K-Infowar.pdf], March 2003.

25. Leonhard, Robert R., *The Principles of War for the Information Age*, Presidio Press Inc., Novato, California, 2000.

26. Montagu, Ewen, *The Man Who Never Was: World War II's Boldest Counter-Intelligence Operation*, United States Naval Institute Press, March 2001.

27. McClure, Scambray, and Kurtz, *Hacking Exposed: Network Security Secrets and Solutions, Third Edition*, McGraw-Hill, New York, 2001.

28. Schleher, D. Curtis, *Electronic Warfare in the Information Age*, Artech House Inc., Boston, Massachusetts, 1999.

29. Sun Tzu, *The Art of War*, Oxford University Press, New York, 1963.

30. White House, *The National Strategy to Secure Cyberspace*, White House, Washington, D.C., February 2003.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Department of the Navy
   Office of the Chief of Naval Operations (N39)
   Arlington, Virginia

4. Naval Network Warfare Command
   NAB Little Creek
   Norfolk, Virginia

5. Fleet Information Warfare Center
   NAB Little Creek
   Norfolk, Virginia

6. Dr. Dan C. Boger
   Naval Postgraduate School
   Monterey, California

7. Dr. Raymond Buettner
   Naval Postgraduate School
   Monterey, California